UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/058,661	01/28/2002	James F. Riordan	CH9-2000-0011	8370

29683 7590 10/31/2006

HARRINGTON & SMITH, LLP
4 RESEARCH DRIVE
SHELTON, CT 06484-6212

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 10/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/058,661	RIORDAN ET AL.	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 August 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed August 9, 2006, have been fully considered.

2. Claims 1-13 are pending and have been examined.

Response to Amendment

3. Applicant's arguments, see Appeal Brief, filed August 9, 2006, with respect to the rejection(s) of claim(s) 1-13 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection under 35 U.S.C. 102(b) (see below, and MPEP 706.02 , V, C) is made in view of Riordan et al. (NPL "Target naming and Service Apoptosis", hereinafter Riordan). It is respectfully noted that this prior art reference was not included in an Information Disclosure Statement.

4. In view of the appeal brief filed on August 9, 2006, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37.

The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

5. A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claim 13 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

8. Claim 13 states "computer program comprising program code...". A computer program per-se is considered non-statutory subject matter according to the MPEP, 2106, paragraph IV.B:

> "Since a computer program is merely a set of instructions capable of being executed by a computer, the computer program itself is not a process and Office personnel should treat a claim for a computer program, without the computer-readable medium needed to realize the computer program's functionality, as nonstatutory functional descriptive material. When a computer program is claimed in a process where the computer is executing the computer pro-gram's instructions, Office personnel should treat the claim as a process claim. See paragraph IV.B.2(b), below. When a computer program is recited in conjunction with a physical structure, such as a computer memory, Office personnel should treat the claim as a product claim. See paragraph IV.B.2(a), below".

9. To expedite a complete examination of the application, the claims rejected under 35 U.S.C. 101 (non-statutory) above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 1-13 are rejected under 35 U.S.C. 102(b) as being anticipated by Riordan.

Regarding claim 1, Riordan teaches a cryptographic system (1) comprising

- first cryptographic algorithm means (2) for enabling cryptographic operations **(pages 222-223)**,
- input/output means (3, 4) for receiving input streams and sending output streams wherein said input streams are transformed to said output streams by said cryptographic operations **(pages 222-223)**,
- at least one test plaintext P_i and for each test plaintext P_i a corresponding test ciphertext C_i **(pages 220-221)**,
- receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i **(pages 222-223)**,
- checking means (6) for checking whether said at least one test ciphertext Ci is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i **(pages 222-224)**,

- Switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm means (2), wherein said stopping by said switching means (7) is triggered by said checking means (6) **(page 223)**.

Regarding claim 5, Riordan teaches a method for creating a cryptographic system (1) for carrying out cryptographic operations characterized by the steps of

- implementing within said cryptographic system (1) a first cryptographic algorithm enabling said cryptographic operations **(pages 222-223)**,
- selecting at least one test plaintext P_i and enciphering each test plaintext Pi with said first cryptographic algorithm and with a corresponding apoptosis key K_i thereby generating a corresponding test ciphertext C_i for each test plaintext P_i **(pages 222-223)**,
- implementing within said cryptographic system (1) said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i **(pages 220-221)**,
- implementing within said cryptographic system (1) receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i **(pages 220-224)**,
- implementing within said cryptographic system (1) checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i

under said first cryptographic algorithm when using said apoptosis key K_i **(pages 222-224)**,

- implementing within said cryptographic system (1) switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm, wherein said stopping by said switching means (7) is triggered by said checking means (6) **(page 223)**.

Regarding claim 8, Riordan teaches a method for operating a cryptographic system (1) for carrying out cryptographic operations characterized by the steps of

- providing a first cryptographic algorithm for enabling said cryptographic operations **(pages 222-223)**,
- receiving input streams and sending output streams wherein said input streams are transformed to said output streams by said cryptographic operations **(pages 222-223)**,
- receiving a control stream which is including at least one apoptosis key K_i **(pages 222-223)**,
- checking whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i **(pages 222-224)**,
- stopping said cryptographic operations with said first cryptographic algorithm **(page 223)**,

- if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i **(page 223)**.

Regarding claim 11, Riordan teaches a computer software product for operating a cryptographic system (1) for carrying out cryptographic operations, said product is characterized by a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, enable the computer to

- perform a first cryptographic algorithm that is enabling said cryptographic operations **(pages 222-223)**,
- receive input streams and send output streams wherein said input streams are transformed to said output streams by said cryptographic operations **(pages 222-223)**,,
- receive a control stream which is including at least one apoptosis key K_i **(pages 222-223)**,
- check whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i **(page 223)**,
- stop said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i **(page 223)**.

Regarding claims 2, 6, 9, and 12, Riordan teaches wherein said cryptographic system (1) includes at least one second cryptographic algorithm means (8) wherein said switching means (7) enables switching to said at least one second cryptographic algorithm means (8) **(pages 222-223)**.

Regarding claims 3 and 10, Riordan teaches

- wherein said receiving means (5) is made for accepting control streams which include at least one plaintext P_i, for each plaintext P_i a corresponding ciphertext C_i and a corresponding apoptosis key K_i **(sections 3 and 4)** and
- said checking means (6) is made for trying to find a test plaintext P_i and a test ciphertext C_i equal to said received plaintext P_i, wherein said checking is done with said apoptosis key of said equal test plaintext P_i and said equal test ciphertext C_i **(section 4.3)**.

Regarding claim 4, Riordan teaches a cascaded list of different cryptographic algorithm means **(page 223)**.

Regarding claim 7, Riordan teaches publishing said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i **(section 4.4)**.

Regarding claim 13, Riordan teaches computer program comprising program code means for performing the steps of claim 8 when said program is run on a computer **(section 4)**.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

13. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

14. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DGC

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100